

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/018491

International filing date: 10 December 2004 (10.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-261033
Filing date: 08 September 2004 (08.09.2004)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

13.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 9 月 8 日
Date of Application:

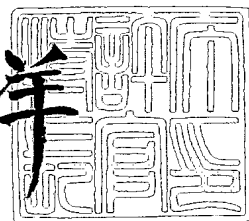
出 願 番 号 特 願 2 0 0 4 - 2 6 1 0 3 3
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 2 6 1 0 3 3]

出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):

2 0 0 5 年 1 月 2 8 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 2054061310
【提出日】 平成16年 9月 8日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/08
H04L 29/06
H04N 5/91

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 森岡 芳宏

【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社

【代理人】
【識別番号】 100097445
【弁理士】
【氏名又は名称】 岩橋 文雄

【選任した代理人】
【識別番号】 100103355
【弁理士】
【氏名又は名称】 坂口 智康

【選任した代理人】
【識別番号】 100109667
【弁理士】
【氏名又は名称】 内藤 浩樹

【手数料の表示】
【予納台帳番号】 011305
【納付金額】 16,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

送信手段と受信手段の間でデータの packets 通信を行なう packets 送受信系において、

A V データの入力端子種別の検出手段と、

前記 A V データと非 A V データとをそれぞれ入力するデータ入力手段と、

前記非 A V データまたは前記 A V データの少なくとも一方より前記 A V データの属性情報を検出し、前記 A V データの暗号化モード情報を生成する手段と、

前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、

packets ヘッダー付加手段とを具備する packets 送受信手段において、

前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、

前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段と

前記 A V データの入力端子種別の検出手段により検出され判別された入力端子種別情報と前記 A V データの属性情報の少なくとも一方の情報をを用いて、前記送信手段と前記受信手段の間での前記 A V データの伝送プロトコルを決定する手段を具備する packets 送信装置。

【請求項 2】

前記暗号化データ生成手段内の前記暗号化手段は暗号化に際して暗号化鍵を使用し、前記送信手段と前記受信手段が規定の条件を具備していることを検証し認証が行われた後に暗号化鍵が前記送信手段と前記受信手段で共有され、規定の伝送条件により前記暗号化鍵が更新されることを特徴とする請求項 1 記載の packets 送信装置。

【請求項 3】

前記暗号化データ生成手段内の認証手段において、

前記送信手段と前記受信手段との間で認証を実行するモードと認証を実行しないモードを持ち、どちらのモードにおいても前記暗号化情報ヘッダー付加手段において前記暗号化モード情報をを用いて暗号化情報ヘッダーを付加することを特徴とする請求項 2 記載の packets 送信装置。

【請求項 4】

前記認証手段において認証を実行するモードは、前記外部より入力される制御情報により決定することを特徴とする請求項 3 記載の packets 送信装置。

【請求項 5】

前記外部より入力される制御情報または認証用の T C P ポート情報は、コンテンツ毎にアクセス位置を指定する U R I、または、Q u e r y により拡張された U R I 情報とにより与えられることを特徴とする請求項 4 記載の packets 送信装置。

【請求項 6】

前記外部より入力される制御情報または認証用の T C P ポート情報は、コンテンツ毎にアクセス位置を指定する U R I で要求されたコンテンツの情報の返信時に与えることを特徴とする請求項 4 記載の packets 送信装置。

【請求項 7】

前記認証手段において認証を実行するモードは、

前記入力 A V データより抽出した制御情報より決定することを特徴とする請求項 3 記載の packets 送信装置。

【請求項 8】

前記認証手段において認証を実行するモードは、

前記外部より入力される制御情報および前記入力 A V データの双方により決定することを特徴とする請求項 3 記載の packets 送信装置。

【請求項 9】

前記 A V データに関するコピー制御情報により前記暗号化情報ヘッダーを付加するかどうかを決定するヘッダー付加制御手段を具備することを特徴とする請求項 3 から 8 記載のパケット送信装置。

【請求項 1 0】

前記 A V データがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合、または、前記 A V データが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には、前記暗号化情報ヘッダーを付加せず、
前記 A V データが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合、または、前記 A V データが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には、前記暗号化情報ヘッダーを付加することを特徴とする請求項 9 記載のパケット送信装置。

【請求項 1 1】

前記コピーフリーコンテンツを放送する放送チャネルは、アナログ放送である VHF、UHF、または B S アナログ放送の放送チャネルであることを特徴とする請求項 1 0 記載のパケット送信装置。

【請求項 1 2】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、および E P N フラグ付きコピーフリーのうち少なくとも 1 つのモードを含んでいることを特徴とする請求項 1 0 記載のパケット送信装置。

【請求項 1 3】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルは、デジタル放送である B S デジタル放送、地上波デジタル放送、または C S デジタル放送の放送チャネルであることを特徴とする請求項 1 0 記載のパケット送信装置。

【請求項 1 4】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信装置または受信ユーザであることを認証された場合に行われることを特徴とする請求項 1 3 記載のパケット送信装置。

【請求項 1 5】

前記認証は、日本のデジタル衛星放送の B-CAD カード、または米国の C A T V 放送で使用される P O D カードなどのセキュリティモジュールによる認証であることを特徴とする請求項 1 4 記載のパケット送信装置。

【請求項 1 6】

前記暗号化手段は前記暗号化情報ヘッダーを、前記 A V データがフリーコンテンツの場合には付加しない、または、前記 A V コンテンツの意味のあるデータ単位毎に付加することを特徴とする請求項 3 から 8 記載のパケット送信装置。

【請求項 1 7】

A V データと非 A V データとをそれぞれのデータバッファに入力し、前記 2 つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力することを特徴とする請求項 1 から 1 6 記載のパケット送信装置。

【請求項 1 8】

前記優先制御の方法は、前記非 A V データが前記データバッファでオーバーフローしない様に制御しながら、前記 A V データを前記データバッファから優先して出力することを特徴とする請求項 1 7 記載のパケット送信装置。

【請求項 1 9】

前記前記 A V データの伝送プロトコルで T C P プロトコルを用いる場合は、T C P コネクションを永続的接続にすることを特徴とする請求項 1 から 1 8 記載のパケット送信装置。

【請求項 2 0】

前記暗号化鍵を共有するための認証と鍵交換方式は、D T C P 方式であることを特徴とす

る請求項 1 から 19 記載のパケット送信装置。

【請求項 21】

前記暗号化鍵の ID 情報または更新情報として整数値を前記暗号化情報ヘッダーまたはパケットヘッダーに付加することを特徴とする請求項 20 記載のパケット送信装置。

【請求項 22】

パケットヘッダー付加手段から出力されるパケットを HTTP プロトコルで伝送する場合、HTTP パケットのパケット毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項 21 記載のパケット送信装置。

【請求項 23】

パケットヘッダー付加手段から出力されるパケットを HTTP プロトコルで伝送する場合、TCP プロトコルが切断して再コネクションを張る毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項 21 記載のパケット送信装置。

【請求項 24】

前記暗号化モードの変化は TCP プロトコルまたは UDP プロトコルのポート番号の変化で検出して設定することを特徴とする請求項 20 記載のパケット送信装置。

【請求項 25】

前記暗号化モードの情報をパケット内に持つことを特徴とする請求項 20 記載のパケット送信装置。

【請求項 26】

前記 AV データのパケット化は、RTP、UDP、IP プロトコルで行うことを特徴とする請求項 1 から 25 記載のパケット送信装置。

【請求項 27】

前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項 26 記載のパケット送信装置。

【請求項 28】

前記 AV データのパケット化は、ハードウェアで行うことを特徴とする請求項 26 記載のパケット送信装置。

【請求項 29】

マルチキャスト伝送の場合、前記暗号化情報ヘッダーを付加したパケットと付加しないパケットの両方を出力することを特徴とする請求項 26 記載のパケット送信装置。

【請求項 30】

前記 AV データを前記 RTP、UDP、IP プロトコルによる IP パケット化の前に、フォワードエラーコレクション (FEC) による誤り訂正を付加することを特徴とする請求項 26 記載のパケット送信装置。

【請求項 31】

前記フォワードエラーコレクション (FEC) はリードソロモン方式またはパリティ方式であることを特徴とする請求項 26 記載のパケット送信装置。

【請求項 32】

前記暗号化情報ヘッダーを付加する場合は、前期 RTP プロトコルにおいて定義されているマーカービット (M ビット) を有効状態にアサートすることを特徴とする請求項 26 記載のパケット送信装置。

【請求項 33】

前記 AV データのパケット化は、HTTP、TCP、IP プロトコルで行うことを特徴とする請求項 1 から 25 記載のパケット送信装置。

【請求項 34】

前記パケット化において、HTTP プロトコルはチャンク伝送方式で行ない、HTTP パケットのペイロード長を前記送信手段で決定して伝送することを特徴とする請求項 33 記載のパケット送信装置。

【請求項 35】

前記H T T Pパケットのペイロード長は、前記暗号化情報ヘッダー長と前期A Vデータを構成するT SまたはタイムスタンプつきT Sの整数倍値を加算した長さであることを特徴とする請求項34記載のパケット送信装置。

【請求項36】

前記パケット化において、前記H T T Pは前記受信手段からのレンジリクエストまたはデータ取得コマンドを受けて前記A Vデータまたは前記暗号化モード情報のうち少なくとも一方を含んだペイロードデータを伝送することを特徴とする請求項33記載のパケット送信装置。

【請求項37】

前記レンジリクエストまたはデータ取得コマンドは、前記送信側における前記A VデータがM P E Gの場合、M P E Gストリームにおける不連続発生連続性情報、前記A Vデータのファイル内におけるM P E GのIピクチャーまたはPピクチャーまたはBピクチャーの位置情報、前記M P E GのIピクチャーまたはPピクチャーまたはBピクチャーの時刻情報、或るIピクチャーから次のIピクチャーの間に存在するPピクチャーとBピクチャーの各個数または合計個数の内、少なくとも1つの情報を参照して実行することを特徴とする請求項36記載のパケット送信装置。

【請求項38】

前記A Vデータのファイル内におけるM P E GのIピクチャーまたはPピクチャーまたはBピクチャーの位置情報または時刻情報は、前記A Vデータが複数の異なるフォーマットであった場合にもオリジナルに持っている複数のIピクチャーまたはPピクチャーまたはBピクチャーの位置情報または時刻情報より、複数の異なるフォーマット間で共通なIピクチャーまたはPピクチャーまたはBピクチャー位置情報または時刻情報を生成し、この共通のIピクチャーまたはPピクチャーまたはBピクチャー位置情報または時刻情報を用いて前記A Vデータのファイル内におけるM P E GのIピクチャーまたはPピクチャーまたはBピクチャーの位置情報または時刻情報の参照情報とすることを特徴とする請求項37記載のパケット送信装置。

【請求項39】

前記A Vデータのパケット化は、受信側のA Vデータ出力がディスプレイ充てに出力されて蓄積されない場合はR T Pが用い、受信側のA Vデータ出力が記録メディアに蓄積される場合はH T T Pを用いられる様に、受信側からの制御により、R T PまたはH T T Pプロトコルで行うことを切替え制御することを特徴とする請求項26または33記載のパケット送信装置。

【請求項40】

前記A Vデータは、S M P T E 259M規格で規定された非圧縮S D方式信号、または、S M P T E 292M規格で規定された非圧縮H D形式、または、I E C 61883規格で規定されたI E E E 1394によるD Vまたはデジタル放送のM P E G-T Sの伝送ストリーム形式、または、D V B規格A O 10で規定されたD V B-A S IによるM P E G-T S形式、または、M P E G-P E S、M P E G-E S、M P E G4、I S O/I E C H. 264の内のいずれか一つのデータストリーム形式を含むことを特徴とする請求項26から39記載のパケット送信装置。

【請求項41】

前記A Vデータを構成するデータブロックにタイムスタンプを付加し、1つ以上のタイムスタンプ付データブロックをまとめてR T PまたはH T T P上にマッピングすることを特徴とする請求項40記載のパケット送信装置。

【請求項42】

前記A VデータがM P E G-T Sの場合、各T Sパケットにタイムスタンプを付加し、複数のタイムスタンプ付T SパケットをまとめてR T PまたはH T T P上にマッピングすることを特徴とする請求項41記載のパケット送信装置。

【請求項43】

前記各T Sパケットに付加するタイムスタンプのクロックはM P E Gのシステムクロック

周波数に等しいことを特徴とする請求項 4 2 記載のパケット送信装置。

【請求項 4 4】

前記 T S パケットに付加されたタイムスタンプより、M P E G - T S のネットワーク伝送により P C R に付加した伝送ジッターを除去して、受信側での M P E G システムクロックの再生を行うことを特徴とする請求項 4 3 記載のパケット送信装置。

【請求項 4 5】

N を 2 以上の整数とした場合、U D P プロトコルまたは T C P プロトコルの N 個のポートを用いて、N 個のフォーマットの A V データをそれぞれのポート毎に割り当てて伝送することを特徴とする請求項 4 0 記載のパケット送信装置。

【請求項 4 6】

U D P プロトコルまたは T C P プロトコルの単一のポートを用いて、複数のフォーマットの A V データを多重して伝送することを特徴とする請求項 4 0 記載のパケット送信装置。

【請求項 4 7】

N を 2 以上の整数、また、M を N より大きい整数とした場合、U D P プロトコルまたは T C P プロトコルの M 個のポートを用いて、N 個のフォーマットの A V データを単一または多重して M 個のポートに割り当てて伝送することを特徴とする請求項 4 0 記載のパケット送信装置。

【請求項 4 8】

複数の A V データを同時に伝送する場合、高データレートの A V データは U D P プロトコルで伝送し、低データレートの A V データは T C P プロトコルで伝送することを特徴とする請求項 4 0 記載のパケット送信装置。

【請求項 4 9】

複数の A V データを同時に伝送する場合、高データレートの A V データより、低データレートの A V データを優先して伝送することを特徴とする請求項 4 0 記載のパケット送信装置。

【請求項 5 0】

前記 A V データの伝送範囲を制限することを特徴とする請求項 2 6 から 3 記載のパケット送信装置。

【請求項 5 1】

前記 A V データの伝送範囲を制限は、I P プロトコルの T T L (T i m e t o L i v e) の値を用いて制限することを特徴とする請求項 5 0 記載のパケット送信装置。

【請求項 5 2】

前期前記 A V データの伝送範囲を制限は、I P パケットの R T T (R o u n d T r i p T i m e) の値を用いて制限することを特徴とする請求項 5 0 記載のパケット送信装置。

【請求項 5 3】

前記 A V データの伝送範囲を制限は、M A C 層のヘッダー情報により制限することを特徴とする請求項 5 0 記載のパケット送信装置。

【請求項 5 4】

前記 I P パケットのパケットサイズは前期送信手段と受信手段の間の I P ネットワークのパス M T U サイズ以下に設定することを特徴とする請求項 2 6 から 3 9 記載のパケット送信装置。

【請求項 5 5】

前記 I P パケットの伝送は、I E E E 8 0 2 . 3 で規定された伝送方法により行われることを特徴とする請求項 2 6 から 3 9 記載のパケット送信装置。

【請求項 5 6】

前記 I P パケットの伝送は、I E E E 8 0 2 . 1 1 で規定された伝送方法により行われることを特徴とする請求項 2 6 から 3 9 記載のパケット送信装置。

【請求項 5 7】

前記 I E E E 8 0 2 . 1 1 の使用において、W E P または W P A またはその他のネット

ワーク接続制限手段を用いることを特徴とする請求項 56 記載のパケット送信装置。

【請求項 58】

前記 IP パケットの伝送は、IEEE 802.1Q により規定された伝送方法により行われることを特徴とする請求項 26 から 39 記載のパケット送信装置。

【請求項 59】

前記 IP パケットの伝送は、IP バージョン 4、または、IP バージョン 6 を使用して行われることを特徴とする請求項 26 から 39 記載のパケット送信装置。

【請求項 60】

前記 IP バージョン 4 を用いる場合、TOS フィールドを用いて優先制御を行なうことを特徴とする請求項 57 記載のパケット送信装置。

【請求項 61】

前記 IP バージョン 6 を用いる場合、Priority フィールドを用いて優先制御を行なうことを特徴とする請求項 59 記載のパケット送信装置。

【書類名】 明細書

【発明の名称】 パケット送信装置

【技術分野】

【0001】

本発明は、IEEE 802.3などのイーサネット（登録商標）（有線LAN）やIEEE 802.11などの無線LANなどを用いて、暗号化されたAVストリームをIPパケット化して高品質に送信するパケット送信装置に関する。

【背景技術】

【0002】

従来、一般家庭において、IEEE 1394を用いて、IEC 61883-4で規定された方式に基づきMPEG-TS信号の暗号化伝送が行なわれている。MPEG-TSなどAVデータを暗号化して伝送する方式の一例として、DTCP (Digital Transmission Content Protection) 方式が規定されている。DTCPは、IEEE 1394やUSBなどの伝送メディア上のコンテンツ保護技術である。DTCP方式は、DTLA (Digital Transmission Licencing Administrator) で規格化された方式であり、HYPERLINK "http://www.dtcp.com" http://www.dtcp.com、HYPERLINK "http://www.dtcp.com/data/dtcp#tut.pdf" http://www.dtcp.com/data/dtcp#tut.pdf、HYPERLINK "http://www.dtcp.com/data/wp#spec.pdf" http://www.dtcp.com/data/wp#spec.pdfや、書籍「IEEE 1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」、133～149ページで説明されている。

【0003】

図9は、DTCP方式を用いたMPEG-TSのIEEE 1394での伝送の一例である。DTCP方式では、送信側をソース901、受信側をシンク902と呼び、暗号化したMPEG-TSなどのコンテンツをソース901からネットワーク903を介して、シンク902へ伝送している。なお、図9に、補足情報として、ソース機器およびシンク機器の例を併記する。

【0004】

次に、図10を用いて、DTCP方式における従来のパケット通信手段の概略を説明する。図10は図9のソース901、およびシンク902の構成の概略図である。まず、DTCP方式に準拠した認証と鍵交換 (Authentication and Key Exchange、AKEと略する) が行なわれる。AKE手段1001に対して、その認証と鍵交換設定情報が入力され、この情報がパケット化手段1002により規定のヘッダーを付加されパケット化され、ネットワーク1007に出力される。ここで、パケット化手段1002は送信条件設定手段1003により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワーク1007より入力する信号がパケット受信手段1004でパケットヘッダーなどの識別によりフィルタリングされ、AKE手段1001に入力される。これにより送信側 (ソース) のAKE手段と、受信側 (シンク) のAKE手段がネットワーク1007 (図9においてはネットワーク903) を介してお互いにメッセージの通信ができる。すなわち、DTCP方式の手順に従い、認証と鍵交換を実行する。

【0005】

送信側 (ソース) と、受信側 (シンク) で認証と鍵交換が成立すれば、次に、AVデータの伝送を行なう。ソースでは、MPEG-TS信号を暗号化手段1005に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段1002に入力し、ネットワーク1007に出力する。シンクでは、ネットワーク1007より入力する信号がパケット受信手段1004でパケットヘッダーなどの識別によりフィルタリングされ、復号手段1006に入力され、復号されMPEG-TS信号が出力される。

【0006】

次に、図11を用い上記手順を補足説明する。図11において、ソースとシンク間はI

IEEE 1394で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクはD T C P所定の処理により認証鍵の共有を図る。そして、ソースは認証鍵を用いて交換鍵を暗号化してシンクに送り、シンクで交換鍵が復号される。ソースでは暗号鍵を時間的に変化させるために、時間的に変化するシード情報を生成し、シンクに送信する。ソースでは、交換鍵とシード情報より暗号化鍵を生成して、M P E G-T Sをこの暗号化鍵を用いて暗号化手段で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化されたM P E G-T S信号を復号する。

【0007】

図12は、図10においてM P E G-T S信号を伝送する場合のIEEE 1394アイソクロナスパケットの一例である。このパケットは、4バイト（32ビット）のヘッダー、4バイト（32ビット）のヘッダーCRC、224バイトのデータフィールド、4バイト（32ビット）のトレイラによって構成されている。暗号化されて伝送されるのは224バイトのデータフィールドを構成するC I PヘッダーとT S信号のうち、T S信号のみで、他のデータは暗号化されない。ここで、D T C P方式固有の情報は、コピー保護情報である2ビットのE M I（Encryption Mode Indicator）、およびシード情報のL S BビットであるO / E（Odd/Even）であり、これらは上記32ビットのヘッダー内に存在するため暗号化されずに伝送される。

【特許文献1】特開2000-59463号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、上記従来の構成では以下のような問題点を有していた。従来のD T C P方式はIEEE 1394において、アイソクロナスパケットを用いて伝送するためM P E G-T S信号のリアルタイム伝送ができるが、インターネットの標準プロトコルであるI Pプロトコルを用いて、イーサネット（登録商標）（IEEE 802.3）、無線LAN（IEEE 802.11）や、その他のI Pパケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。

【0009】

すなわち、I Pプロトコルを介して論理的に接続された送信機器と受信機器の間を、地上波／B Sデジタル放送やサーバー型放送などデジタル著作権保護対応のコンテンツを著作権保護しつつ伝送できないという大きな問題点がある。

【0010】

また、ライブ放送の伝送において、H T T Pプロトコルを用いる場合、H T T Pリクエストの度に、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長を受信側で計算する必要があり、受信側の処理が重いという課題がある。

【0011】

さらに、ハードディスクなどに蓄積されたコンテンツを早送り、巻き戻し、スロー再生などの特殊再生の簡単に実現することが困難であるという問題点がある。

【0012】

さらに、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツを共通の方法で簡単に、早送り、巻き戻し、スロー再生などの特殊再生することが困難であるという問題点がある。

【課題を解決するための手段】

【0013】

上記課題を解決するために、本願第1の発明は、課金処理などを含むR M Pなどのデジタル著作権対応のA Vデータおよび非A Vデータとをそれぞれ入力するデータ入力手段と

、前記データ入力手段の出力を入力し、入力されるデジタル著作権規定より暗号化伝送モードを選択できる手段を具備する。すなわち、「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段とを具備する。

【0014】

これにより、課金処理などを含むRMP情報などデジタル著作権対応のMP E G-T S信号などのAVストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加することを決めることにより、送受信機器間での信号の互換性を確保しながら、AVストリームの秘匿性を保つことが可能となる。

【0015】

本願第2の発明は、第1の発明において、ライブで放送されているコンテンツをHTT Pのチャック伝送方式で伝送することにより、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長HTT Pリクエストの度に、受信側（クライアント）で計算する必要がなくなり、受信側の処理を軽くすることができる。

【0016】

本願第3の発明は、第1の発明において、ハードディスクなどに蓄積されたコンテンツをHTT Pのレンジリクエストを用いて伝送することにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現することができる。

【0017】

さらに、本願第4の発明は、第3の発明において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの異なるI、P、Bピクチャのバイト位置情報、時刻情報より、共通フォーマットとしてのI、P、Bピクチャフレーム位置情報を生成することにより、高品質なスロー再生、早送り、巻き戻しなどの特殊再生を容易に実現することが可能となる。

【発明の効果】

【0018】

本願第1の発明によれば、以下のような効果を有する。すなわち、地上波放送、衛星放送、CATVやインターネット経由で受信するデジタル放送信号より検出、抽出できるAVコンテンツの属性情報を送信端末と受信端末間でUP n P-AVやHTT Pなどのデータ交換プロトコルを用いて伝送することにより、送信端末と受信端末間でのAVコンテンツを送信する場合の暗号化モード、コンテンツ属性情報の伝送方法を決めることができる。さらに、暗号化情報ヘッダーの付加ルールを決められるため、送受信機器間でのAVストリームの秘匿性を保ちながら信号の互換性を確保することが可能となる。

【0019】

また、本願発明によれば、ネットワークを用いたAVコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（AVデータコンテンツ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるAVデータの販売、課金が可能となり、安全性の高いB-B、B-Cのコンテンツ販売流通が可能となる。

【0020】

また、本願発明によれば、AVコンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通りCPUを用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データであるAVデータに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価

なCPUや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

【0021】

そこで、本願発明によれば、サーバー型放送のRMPで用いる課金情報などを含むRMPで視聴あるいはコピー制限されたコンテンツをRMPに対応していないクライアントにCNM(Copy No More)やCN(Copy Never)で見せることができ、サーバー型放送の普及を加速することができる。

【0022】

本願第2の発明によれば、以下のような効果を有する。すなわち、ライブで放送されているコンテンツをHTTPのチャンク伝送方式で伝送することにより、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長HTTPリクエストの度に、受信側(クライアント)で計算する必要がなくなり、受信側の処理を軽くできる。

【0023】

本願第2の発明によれば、以下のような効果を有する。すなわち、ハードディスクなどに蓄積されたコンテンツをHTTPのレンジリクエストを用いて伝送することにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現できる。

【0024】

さらに、本願第4の発明は、第3の発明において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの異なるIフレーム位置情報より、共通のIフレーム位置情報を生成することにより、簡単に、早送り、巻き戻し、スロー再生などの特殊再生することを実現する。

【発明を実施するための最良の形態】

【0025】

最初に本願発明の位置付けを明確にするために適用されるシステム例の概略について説明する。図1は本願発明を適用するシステムの一例である。

【0026】

図1において、送信機器101および受信機器103は、本願第1, 2, 3, 4および5の発明実施部である(以下、本願発明部)。101は送信機器、102はルータ、103は受信機器である。送信機器101には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム(MPEG-TSなどコンテンツ)が入力され、以下の手順1から3に基づき、通信が実行される。

【0027】

<手順1>送受信パラメータの設定を行なう。

【0028】

(手順1-1)送受信機器のMACアドレス、IPアドレス、TCP/UDPポート番号等を設定。

【0029】

(手順1-2)送信信号の種別、帯域を設定。QoSエージェントとして動作する送信機器101と受信機器103、QoSマネージャとして動作するルータ102との間でIEEE 802.1Q(VLAN)規格を用いたネットワークの運用に関する設定を実施。

【0030】

(手順1-3)優先度の設定(IEEE 802.1Q/pによる運用)

<手順2>認証と鍵交換：

(手順2-1)認証と鍵交換を行なう。たとえば、DTCP方式を用いることもできる。

【0031】

<手順3>ストリーム伝送：

(手順3-1)送信機器と受信機器間での暗号化されたストリームコンテンツ(MPEG-TS)の伝送

なお、コンテンツの入力信号としてMPEG1/2/4などにおけるMPEG-TS、MPEG-PS、MPEG-ES、MPEG-PESなどがある。

【0032】

ここでは、例ではMPEG-TSを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム（ISO/IEC 13818）、DV（IEC 61834、IEC 61883）、SMPTE 314M（DV-based）、SMPTE 259M（SDI）、SMPTE 305M（SDTI）、SMPTE 292M（HD-SDI）等で規格化されているストリーム、さらには、一般的なAVコンテンツも適用可能である。

【0033】

さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。

【0034】

次に、上記手順2の認証と鍵交換に関して補足説明する。図2において、送信機器と受信機器間はIPネットワークにより接続されている。まず、送信機器から受信機器へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。

【0035】

受信機器は、コンテンツのコピー保護情報の解析を行い、使用する認証方式を決定して認証要求を送信機器に送る。

【0036】

これらの処理を通して送信機器と受信機器は認証鍵を共有する。

【0037】

次に、送信機器は認証鍵を用いて交換鍵を暗号化して受信機器に送り、受信機器で交換鍵が復号される。

【0038】

送信機器では暗号鍵を時間的に変化させるために、時間的に変化する鍵変更情報を生成し、受信機器に送信する。

【0039】

送信機器では、交換鍵と鍵変更情報より暗号化鍵を生成して、MPEG-TSをこの暗号化鍵を用いて暗号化手段で暗号化して受信機器に送信する。

【0040】

受信機器は受信した鍵変更情報を交換鍵より復号鍵を復元する。受信機器ではこの復号鍵を用いて暗号化されたMPEG-TS信号を復号する。

【0041】

図3は本方式をイーサネット（登録商標）を用い2階建ての家庭に適用した場合の一例である。

【0042】

図3において、301は1階のネットワーク構成、302は2階のネットワーク構成である。

【0043】

303は1階に設置されインターネットと接続されるルータ、304は2階に設置されているスイッチングハブである。

【0044】

304はルータ303とスイッチングハブ304を接続するイーサネット（登録商標）ネットワークである。家庭内の全てのイーサネット（登録商標）ネットワークの帯域は100Mbpsである。

【0045】

1階のネットワーク構成の詳細としては、ルータ303にはテレビ（TV）、パソコン

(PC)、DVDレコーダが100Mbpsのイーサネットで接続され、また、エアコン、冷蔵庫がECHONETで接続されている。

【0046】

また、2階では、スイッチングハブ304にテレビ(TV)、パソコン(PC)、DVDレコーダが100Mbpsのイーサネットで接続され、また、エアコンがECHONETで接続されている。なお、ECHONETは「エコーネットコンソーシアム」(HYPERLINK "http://www.echonet.gr.jp/" http://www.echonet.gr.jp/)で開発されている伝送方式である。

【0047】

図3において、パソコン(PC)、DVDレコーダ、ルータ301およびスイッチングハブ(304)は、IEEE 802.1Q(VLAN)に対応している。すなわち、ルータ(301)およびスイッチングハブ(304)において、各ポートのデータレートが全て同じ(例えば100Mbps)場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ(あるいは、スイッチングハブ)内部で失われず全て出力ポートに出力される。

【0048】

スイッチングハブでは、たとえば8個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

【0049】

図3において、家庭内の全てのイーサネット(登録商標)の帯域が100Mbpsであるため、1階と2階間のネットワーク305の帯域も100Mbpsである。

【0050】

1階と2階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク305上を流れるデータのデータレート合計が100Mbpsを超える可能性があり、MPEG-TSの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。

【0051】

この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。

【0052】

端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。

【0053】

たとえば、MPEG-TSストリームの伝送優先度をファイル転送データの伝送優先度よりも高くすると、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することが可能となる。

【0054】

前述したルータ、またはスイッチングハブにおける伝送速度制限機構は、データ流入制御により実現できる。

【0055】

すなわち、ルータ(あるいは、スイッチングハブ)の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。

【0056】

この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジ

ューリング方式 W F F Q 方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。

【0057】

これらのスケジューリング方式に関する情報は、戸田巖著、「ネットワーク Q o S 技術」、平成 13 年 5 月 25 日（第 1 版）、オーム社刊の第 12 章などに記述されている。

【実施例 1】

【0058】

本願第 1 の発明について説明する。図 4 は本願第 1 の発明のパケット送受信手段に関するブロック図である。

【0059】

401 は入力 A V コンテンツをその関連メタ情報が持つ送信条件に従う暗号化、関連メタ情報の付加、パケット化を行うパケット送受信手段である。

【0060】

ここで、送信条件設定管理手段 403 には、送信データのフォーマット種別、送信先アドレスやポート番号などの送信情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力される。

【0061】

コンテンツはその選択に関して、コンテンツ毎または放送チャネル毎に Q u e r y により拡張された U R I 情報で与える。ここで、U R I に主データ部にコンテンツの U R I 情報、Q u e r y 部にそのコンテンツの認証情報をマッピングする。これにより、もし、Q u e r y 部がなければそのコンテンツの伝送には認証が不必要であり、Q u e r y 部が存在すればそのコンテンツの伝送には認証が必要である様にモード設定することができる。U R I と Q u e r y の例は、例えば下記の形式で与えることができる。

【0062】

<service>: // <host> : <port> / <path> / <filename> . <ext> ? A K E P O R T = <port2>

ここで、<host> : <port> / <path> / <filename> . <ext> は A V コンテンツの U R I とファイル名称を表しており、以下の Q u e r y 部における <port2> は認証用ポート番号を表わす。ここで、一般に認証サーバーとコンテンツ提供サーバーが同一であれば、認証用ポートの I P アドレスは A V コンテンツの I P アドレスと同じであるが、認証サーバーとコンテンツ提供サーバーが異なる場合には認証用ポートの I P アドレスは A V コンテンツの I P アドレスと異なる。送信側はこれら、U R I と Q u e r y で認証の実行モード情報を受信側に与える。受信側は W E B ブラウザや U P n P - A V の C D S （コンテンツディレクトリサービス）を用いて、上記の U R I と Q u e r y 情報を受け取り、認証モードを決定することができる。

【0063】

また、D R M 設定管理手段 404 は、送信条件の設定管理手段 403 または T S ストリーム識別手段より D R M 設定情報を受け取り、その情報を保持、管理するとともに、A K E に必要な関連情報を A K E 手段 405 に引き渡す。ここで、D R M は Digital Rights Management の略であり、デジタル著作権管理のことである。D R M 設定管理手段で、コンテンツ伝送には D R M の課金、購入処理が必要な場合には D R M コンテンツ購入手段（411）によりコンテンツの購入処理が行われる。コンテンツの購入処理が終了後に、コンテンツの C C I （コピー制御情報）が設定され A K E 手段 405 に渡される。

【0064】

ここで、A K E は、「認証と鍵交換」（Authentication and Key Exchange）の略語であり、A K E 手段は認証手段と暗号化鍵の交換手段を具備する。

【0065】

A K E 手段 405 に対して A K E 設定情報を入力し、この A K E 設定情報に関連した情

報、たとえばコピー保護情報と暗号化鍵変更情報、がパケット化手段406に入力され、TCP/IPプロトコルのヘッダーを付加され、さらに、フレーム化手段408においてMAC(Media Access Control)ヘッダーが付加されイーサネット(登録商標)フレームに変換し、送信フレームとしてネットワークに出力される。

【0066】

図4を用いて、DTCP方式による著作権対応のAVコンテンツの伝送ステップの一例について説明する。ここで、DRM対応のAVコンテンツとはデジタル放送のコピー制御や、サーバー型放送(ARIB規格、STD-B38)のRMP方式(RMPI)や、各種のネットワークDRMで扱っているコンテンツ保護情報を表す。

【0067】

(ステップ1) まず、受信側で送信側より、UPnP-AV、CDS(Content Directory service)などで与えられるコンテンツリストより受信したいコンテンツを選択し、ソース側にコンテンツの送信要求を投げる。

【0068】

(ステップ2) コピー制御情報またはDRM情報を含んだデータがTSストリーム識別手段402により抽出され、DRM設定管理手段404経由で、AKE手段405に入力される。

【0069】

DTCP情報としてはAKE手段405よりコンテンツの保護モード情報(EMI情報)が暗号化情報ヘッダー付加手段415に出力され、ヘッダー情報として付加された後、パケット化手段406に入力される。

【0070】

(ステップ3) 受信側(シンク)では、パケット受信手段410よりAKEコマンド受信処理を行うAKE手段405に入力されたコンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。

【0071】

(ステップ4) ソースとシンク間でDTCP所定の処理が行なわれ、認証鍵が共有される。

【0072】

(ステップ5) 次に、ソースはAKE手段405において、認証鍵を用いて交換鍵を暗号化してパケット化手段406を経由してシンクに送り、シンクのAKE手段において交換鍵が復号される。

【0073】

(ステップ6) ソースでは暗号鍵を時間的に変化させるために、暗号化鍵生成手段において、時間的に変化するシード情報(O/E)を生成し、AKE手段405、暗号化情報ヘッダー付加手段415、およびパケット化手段416を経由してシンクに送信する。

【0074】

(ステップ7) ソースでは、暗号化鍵を生成するAKE手段405において交換鍵とシード情報より暗号化鍵を生成して、暗号化手段でMPEG-TSを暗号化してパケット化手段406に出力する。

【0075】

(ステップ8) シンク内部の、暗号鍵変更情報を生成するAKE手段405はパケット受信手段410よりシード情報を受信し、復号鍵を生成するAKE手段405はこのシード情報と交換鍵より復号鍵を復元する。

【0076】

(ステップ9) シンクでは、この復号鍵を用いて復号化手段418において、暗号化されたMPEG-TS信号入力を復号して出力する。

【0077】

ここで、DRMコンテンツがあつて、そのコピー可能回数がN回(Nは2以上の整数)

である場合の動作について説明する。まず、受信端末がDRMに対応している場合には、伝送暗号状態のCCIをCOG（コピー1回可能）またはCNM（コピーノーモア）、またはCN（コピーネバー）に設定して伝送する。

【0078】

ここで、暗号化伝送されるエンベデッドCCIとして「残りのコピー可能回数情報」を（N-1）回として受信側に伝え、受信側で暗号を復号した後に、DRM対応端末では残りのコピー可能回数を（N-1）回に設定する。

【0079】

また、受信端末がDRMに対応していない場合には、コンテンツのDRM情報は削除してNMCのCCIを用いて受信側に伝送する。

【0080】

図4において、AKE手段は暗号化ヘッダー情報を暗号化情報ヘッダー付加手段415に入力し、以下の様に暗号化情報ヘッダー付加制御を行なう。

【0081】

図4において、送信条件の設定管理手段403に入力されるAVデータの関連情報（放送、または蓄積コンテンツ再生の場合）は、たとえば次のような場合が考えられる。

（ケース1）前記AVデータがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合。この様な放送チャネルの例としては、たとえば、アナログ放送であるVHF、UHF、またはBSアナログ放送の放送チャネルがある。

（ケース2）前記AVデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合。この様な放送チャネルの例としては、たとえば、BSデジタル放送の有料チャネルやCATV放送による有料チャネルがある。この一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびEPNフラグ付きコピーフリーが放送内容により時々刻々と切り替わるのが特徴である。

ここで、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信装置または受信ユーザであることを認証された場合に行われるように制御できる。この認証の例としては、日本のデジタル衛星放送のBCASカード、または米国のCATV放送で使用されるPODカードなどのセキュリティモジュールによる認証が考えられる。

【0082】

また、暗号化情報ヘッダーの付加制御は、たとえば以下の様に行なう。すなわち、コピーフリーコンテンツを放送する放送チャネルを受信した場合には付加しない。

【0083】

また、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信した場合には付加する。さらに、AVデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない。

【0084】

そして、AVデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する。

【0085】

以上の様に、暗号化情報ヘッダーの付加制御を行うことにより、著作権者が設定したAVコンテンツのCCI（コピー制御情報）をネットワーク伝送においても継承して伝えていくことができる。

【0086】

さらに、送信側と受信側で暗号化情報ヘッダーの付加制御のルールを揃えることにより異機種間での動作互換性を確保することができる。

【0087】

ここで、パケット化手段406は送信条件の設定管理手段403により決定された送信パラメータにより、入力データのパケット化および送信を行なう。

【0088】

送信条件の設定管理手段403は、送信キュー制御手段407に、送信先アドレスやポート番号などの送信情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件を与える。

【0089】

これらのデータは、TCP/IP処理によるパケット化手段406およびフレーム化手段408で生成するヘッダーやペイロードデータなどを設定する。

【0090】

受信側では、ネットワークより入力する信号がフレーム受信手段409でMACヘッダーを元にフィルタリングされ、IPパケットとしてパケット受信手段410に入力される。パケット受信手段410ではIPパケットヘッダーなどの識別によりフィルタリングを行い、AKE手段405に入力される。これにより送信側のAKE手段と、受信側のAKE手段がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、AKE手段の設定手順に従い、認証と鍵交換を実行することができる。

【0091】

送信側と、受信側で認証と鍵交換が成立すれば、暗号化したAVデータを送信する。

【0092】

送信側では、入力信号が例えばMPEGのフルTSストリームの場合、そのフルTSストリームをTSストリーム識別手段402に入力し、フルTSストリームをパーシャルTSストリームに変換する。

【0093】

そして、変換されたパーシャルTSストリームをコンテンツバッファ413に送り暗号化タイミングの調整を行う。

【0094】

コンテンツバッファ413のパーシャルTS出力を暗号化手段414に入力し暗号化を行ない、前述したEMI、シード情報（シード情報のすべてのビット、または、O/Eなど一部のビット）などのAKE情報を暗号化情報ヘッダー付加手段415で付加する。

【0095】

さらに、この信号をパケット化手段406に入力し、送信キュー制御手段407より与えられる条件を用いてTCP/IPプロトコルのヘッダーを付加する。パケットの優先伝送制御を行うためには、フレーム化手段408において、たとえば、802.1Q（VLAN）方式を用いて、MACヘッダーを付加しイーサネット（登録商標）フレームに変換して、送信フレームとしてネットワークに出力する。ここで、MACヘッダー内のTCI（Tag Control Information）内のPriority（ユーザ優先度）を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

【0096】

受信側では、ネットワークより入力する信号がフレーム受信手段409でMACヘッダーを元にフィルタリングされ、IPパケットとしてパケット受信手段410に入力される。パケット受信手段410でパケットヘッダーなどの識別によりフィルタリングし、送信条件などの伝送関連データは送信条件の条件設定手段417に出力し、AKE関連データはAKE手段405に出力し、AVコンテンツは暗号の復号化手段418に出力する。復号化手段418では、暗号化情報ヘッダーの除去と暗号の復号化が行われ、復号されたMPEG-TS信号が出力される。

【0097】

なお、送信条件設定手段417には、受信状況を送信側にフィードバックするためのデータが入力され、IPパケットのパケット化手段406およびイーサネット（登録商標）フレームのフレーム化手段408で生成するヘッダーおよびペイロードデータを設定する情報を送信条件の設定管理手段403にフィードバックする。

【0098】

次に、図5のプロトコルスタックを用い上記手順を補足説明する。図5の送信側において、まず送信側から受信側へ暗号化されたコンテンツおよび、DRM設定管理手段より与えられるコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求を送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報（機器ID、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせ生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるMPEG-TSは暗号化鍵により暗号化される。そして暗号化されたMPEG-TSは、AVデータとしてTCP（またはUDP）パケットのペイロードとしてTCPパケットが生成される。さらにこのTCPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット（登録商標）MACフレームが生成される。なお、MACとしてはイーサネット（登録商標）であるIEEE 802.3だけでなく、無線LAN規格のIEEE 802.11のMACにも適用できる。

【0099】

さて、イーサネット（登録商標）MACフレームは、イーサネット（登録商標）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（登録商標）MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP（またはUDP）パケットが抜き出される。そして、TCP（またはUDP）パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG-TS（コンテンツ）が復号され出力される。

【0100】

以上、MPEG-TS信号などのAVストリームを送信機器で暗号化して、IPパケットをネットワークにより伝送し、受信機器で元の信号に復号できる。

【0101】

なお、図4においては、送信キュー制御手段407、第1キュー手段としてのAVデータキュー、および第2キュー手段としての一般データキューを具備している。

【0102】

図4において、AKE手段405に対してAKE設定情報を入力され、このAKE設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段406に入力され、TCP/IPプロトコル処理をして、第1キュー手段に入力される。

【0103】

また、送信側ではMPEG-TS信号を暗号化手段414に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段406に入力し、TCP/IPプロトコル処理をして、AVデータキュー手段に入力する。

【0104】

送信キュー制御手段407は、第1キューと第2キューにデータが存在する場合、どちらのデータを優先して出力するかを制御を行なう。通常状態では、一般データよりもMPEG-TSなどのコンテンツデータを優先制御して出力する。たとえば、送受信機器間でMPEG-TSを低レイテンシ（低遅延）で伝送する場合には、MPEG-TS用バッフ

ァも小さくなるため、オーバーフローが発生しやすい。送信側でMPEG-TSバッファがオーバーフローしそうになった場合、あるいは、受信側からフィードバックされた情報を参照して受信側のMPEG-TSのバッファがアンダーフローしそうになったことが判明した場合には、MPEG-TSデータを優先出力する様に第2キュー手段の優先度を更に適応的に上げることにより、これらバッファ破綻を回避できる。

ただし、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くするには、第1キューの優先度を適応的に上げればよいが、これでは前述したMPEG-TSバッファのオーバーフローまたはアンダーフローが発生する可能性がある。

バッファのオーバーフローやアンダーフローを避け、かつ、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くする別手段として、機器制御用パケットだけはキューを経由せずに直接フレーム化手段に出力する方法により、迅速な制御応答が実現できる。あるいは、機器制御用パケットに対して第3キューを新たに用意する方法により、迅速な制御応答が実現できる。

【0105】

なお、図3において、スイッチングハブを用いたネットワークポロジを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。

【0106】

たとえば、1階と2階の間のネットワーク305の帯域を、従来の実施例で説明した100Mbpsから1Gbpsに拡張することによって、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することができる。

【0107】

たとえば、市販されている100Mbpsのポートを8つ、1Gbpsのポートを1つ持ったスイッチングハブを用い、1階と2階を結ぶネットワーク305に1Gbpsのポートを接続し、残りの8chの100MbpsのポートにTVなどのAV機器を接続する。

【0108】

100Mbpsのポートは8つなので、8つのポートのデータがそれぞれ最大100Mbpsで入力されて1Gbpsのポートに出力されたとしても、100Mbps×8ch=800Mbpsと1Gbpsより小さいため、8つのポートから入力されたデータはスイッチングハブ内部で失われず全て1Gbpsのポートに出力される。よって、1階で発生したデータは全て2階に伝送することが可能である。また、逆に2階で発生したデータも全て1階に伝送することが可能である。以上の様に、スイッチングハブを用いる場合、ネットワークポロジを工夫することによりストリーム伝送とファイル転送を共存させることができる。

【0109】

また、図4のAKE手段405に対してAKE設定情報を入力し、このAKE設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段406に入力されプロセッサを用いた内部のソフトウェア処理でTCP/IPプロトコル処理をされ、一般データキューに入力される。

【0110】

送信側ではMPEG-TS信号を暗号化手段414に入力して、MPEG-TS信号を暗号化した後、この暗号化されたMPEG-TS信号をパケット化手段406に入力し、内部のハードウェア処理によりUDP/IPプロトコルの処理をされ、AVデータキューに入力する。

【0111】

送信キュー制御手段407は、第1キューであるAVデータキューと第2キューである一般データキューの双方にデータが存在する場合、前述の実施の形態2と同様に、2つのキューからのデータ出力に関して優先制御を行なう。

【0112】

さて、受信側では、ネットワークより入力する信号がフレーム受信手段409でMACヘッダーを元にIPパケットがフィルタリングされる。ここでは、ソースの上記パケット化手段(406)から出力されたIPパケットが、シンクのパケット受信手段410に入力される。一般データキューで受信したパケットはプロセッサを用いたソフトウェア処理でTCP/IPプロトコルの受信処理を行い、AKE手段(405)または受信条件の設定管理手段417に出力する。また、AVデータキューで受信したパケットはハードウェア処理によりUDP/IPプロトコルの受信処理を行い、暗号化されたAVデータは復号化手段(418)に入力され、暗号復号を行った後にMP EG-TSを出す。

【0113】

なお、送信側から受信側への、EMI、シード情報の伝送方法としては、たとえば、専用の別パケットを生成して伝送することも可能であり、暗号鍵復元がさらに困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなど公衆網において、リアルタイムに伝送されるAVデータの暗号化パラメータが変化させたり、別パケットで送ると、コンテンツの盗聴、漏洩をより困難にすることができる。管理制御データに関しては図5の例と同様に、ソフトウェア処理によりTCPパケットが生成され、IPパケット化される。

【0114】

さて、イーサネット(登録商標)MACフレームは、イーサネット(登録商標)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット(登録商標)MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからUDPパケットが抜き出され、UDPパケットからAVデータが抜き出され、交換鍵とシード情報より復元された復号鍵Kcにより、MP EG-TS(コンテンツ)が復号され出力される。

【0115】

図6は、MP EG-TSをIPパケット化、さらにイーサネット(登録商標)フレーム化して伝送する場合のパケット形式の一例である。188バイトのMP EG-TSに6バイトのタイムコード(TC)を付加して194バイトの単位を作る。TCは42ビットのタイムスタンプと6ビットのベースクロックID(BCID)により構成される。BCIDによりタイムスタンプの周波数情報を表すことができる。たとえば、(ケース1)BCIDが0x00の場合は、タイムスタンプの周波数情報はない、(ケース2)BCIDが0x01の場合は、タイムスタンプの周波数情報としては27MHz(MP EG2のシステムクロック周波数)である、(ケース3)また、BCIDが0x02の場合は、タイムスタンプの周波数情報としては90kHz(MP EG1で使用するクロック周波数)である、(ケース4)BCIDが0x03の場合は、タイムスタンプの周波数情報としては24.576MHz(IEEE 1394で使用するクロック周波数)である、(ケース5)BCIDが0x04の場合は、タイムスタンプの周波数情報としては100MHz(イーサネット(登録商標)で使用する周波数)である、という様にBCIDでタイムスタンプの周波数情報を表すことができる。194バイト単位のデータを2つあわせて暗号化して、更に14バイトの暗号化情報ヘッダーと合わせてRTPプロトコルのペイロードとする。ここで、暗号化情報ヘッダーは、4ビットのEMIと、64ビットのシード情報と12ビットのReserved Dataにより構成される。RTPパケットはUDPおよびIPプロトコルによりパケット化された後、イーサネット(登録商標)フレーム化される。イーサネット(登録商標)ヘッダとしては、図6に示す様に、標準的なイーサネット(登録商標)ヘッダとIEEE 802.1Q(VLAN)により拡張されたイーサネット(登録商標)ヘッダの両方をサポートする。なお、IEEE 802.1Q(VLAN)により拡張されたイーサネット(登録商標)ヘッダにおけるTCIフィールド

の中の3ビットのPriorityフラグにより、イーサネット（登録商標）フレームの優先度を設定することができる。

【0116】

以上により、送受信機器間でMP EG-T S信号を暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。また、データ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで処理できる。

さらに、ハードウェア処理により、受信処理においても、イーサネット（登録商標）フレームを受信して、3層のIPヘッダー、4層のUDPヘッダーを同時に検査することもできる。MP EG-T Sパケットと一般データパケットを分離し、MP EG-T Sパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信ができる。

【0117】

パケットの送信タイミング、あるいは2つの送信データキューからのデータ送信割合をソフトウェアではなくハードウェアで制御するとクロック単位で完全な送出制御が可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

【0118】

以上により、送受信機器間でMP EG-T S信号をD T C P方式により暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで処理できる。

【実施例2】

【0119】

本願第2の発明について説明する。図4は本願第2の発明のパケット送受信手段に関するブロック図である。以下、第1の実施例と同じ部分の説明は省略し、異なる部分のみを説明する。

【0120】

本願第2の発明は、第1の発明において、ライブで放送されているコンテンツをH T T P/R T Pヘッダー付加手段416および、パケット化手段406においてH T T Pのチャック伝送方式で伝送する様に伝送プロトコルを設定する。

【0121】

これにより、従来は、前記暗号化に関して付加するヘッダー長や伝送コンテンツ長H T T Pリクエストの度に、受信側（クライアント）で計算していたが、この計算の必要がなくなり、受信側の処理を軽くできる。H T T Pのペイロードデータ長としては、暗号化される伝送ペイロードの暗号化情報ヘッダーとT Sの整数倍であり、送信側で都合のよい値に設定することができる。このチャック伝送時にはT C Pのコネクションは永続的接続モード（Keep Alive設定）されていると、T C Pコネクションの切断、確立をコンテンツ伝送中にT C Pトランザクション毎に頻繁に行う必要がなくなり効率のよいA V伝送を行うことができる。

【実施例3】

【0122】

本願第3の発明について説明する。図7は本願第3の発明のパケット送受信手段に関するブロック図である。以下、第1の実施例と同じ部分の説明は省略し、異なる部分のみを

説明する。

【0123】

図7においては、TSストリーム識別手段402に接続した蓄積手段701を具備する。ここで、蓄積手段701は、ハードディスクや光ディスクであり、本発明において、第1の発明において、ハードディスクや光ディスクなどに蓄積されたMP EG-TSデータをHTTPのレンジリクエストを用いて伝送する。

このレンジリクエストは、蓄積手段701に蓄積されたMP EG-TSファイルとペアになっているファイル中におけるIフレーム位置情報を含んだファイルである。例えば、DVD-VR方式ではIFOファイルと呼ばれているものである。このIFOファイルと同等のIフレーム位置情報を持ってファイルを用いることにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現することができる。

【0124】

本発明で用いる入力データの適用範囲として、サーバー型放送や各社の異なるDRM方式など一般のDRM対応のAVコンテンツをDTC P-I Pを用いて伝送することが可能となる。

【実施例4】

【0125】

本願第4の発明について説明する。図8は本願第4の発明のパケット送受信手段に関するブロック図である。以下、第3の実施例と同じ部分の説明は省略し、異なる部分のみを説明する。

【0126】

図7においては、蓄積手段701は、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの場合、クライアントは全ての異なるコンテンツのIフレーム位置データを格納したファイルを理解しなければならない。フォーマット数が多くなると、これは受信側にとって大きな負担となるため、送信側で異なるIフレーム位置情報より、共通のIフレーム位置情報生成手段801で共通のIフレーム位置情報を生成する。これにより、各社のHDD記録フォーマット、DVD-VR方式、あるいはBD方式など異なる蓄積フォーマットであっても、簡単に、早送り、巻き戻し、スロー再生などの特殊再生することを実現する。

【0127】

このパケット化において、HTTPは受信手段からのレンジリクエストまたはデータ取得コマンドを受けて前記AVデータまたは前記暗号化モード情報のうち少なくとも一方を含んだペイロードデータを伝送する。このレンジリクエストまたはデータ取得コマンドは、前記送信側における前記AVデータがMP EGの場合、MP EGストリームにおける不連続発生連続性情報、前記AVデータのファイル内におけるMP EGのIピクチャまたはPピクチャまたはBピクチャの位置情報、或るIピクチャから次のIピクチャの間に存在するPピクチャとBピクチャの各個数または合計個数の内、少なくとも1つの情報を参照して実行する。ここで、MP EGストリームにおける不連続発生情報とは、ARIB規格、ARIB-TR-B14またはARIB-TR-B14の第2編に記載されているDIT情報を元に生成することができる。このストリームの不連続点とは、たとえば、MP EGのパーシャルTSの場合、MP EG-TSストリームのシステムタイムベースの不連続が発生する点、たとえば、PCRが不連続になる点、または、パーシャルTSを構成するパケットの内のどれか1つのトランスポートパケットヘッダのcontinuity_counterの不連続が発生する点のことである。

【0128】

また、AVデータのファイル内におけるMP EGのIピクチャまたはPピクチャまたはBピクチャの位置情報は、前記AVデータが複数の異なるフォーマットであった場合にもオリジナルに持っている複数のIピクチャまたはPピクチャまたはBピクチャの位置情報、前記MP EGのIピクチャまたはPピクチャまたはBピクチャの時刻情報より、複数の異なるフォーマット間で共通なIピクチャまたはPピクチャまたはBピクチャ位置情報を

生成し、この共通の I ピクチャまたは P ピクチャまたは B ピクチャ位置情報を用いて前記 AV データのファイル内における MPEG の I ピクチャまたは P ピクチャまたは B ピクチャの位置情報、時刻情報の参照情報とする。これにより、たとえば HDD に、異なる記録フォーマットで記録されている MPEG-TS ファイルがあっても、リモート端末からは共通の I または P または B ピクチャの位置情報や時間情報で特定のピクチャに直接アクセスできるという大きなメリットがある。

【0129】

たとえば、図 13 の一例の様に、パーシャル TS を記録した HDD や BD ディスクなどから、I または P または B ピクチャの連続性およびファイル内での位置情報などを統一した「ピクチャ情報ファイル」にき出す。ネットワークを介して離れた場所に存在する端末からは、この統一されたピクチャ情報ファイルをバイト位置や時刻情報 (timestamp) で参照することにより、異なる TS 記録フォーマットでも各ピクチャ位置をきめ細かに参照することができる。

【0130】

図 13 において、“discont” はパーシャル TS の不連続点を示す 1 ビットのフラグである。たとえば、この値が“0”の時はパーシャル TS は連続であり、“1”の時は不連続を意味する。

【0131】

また、“IPB フラグ”は、2 ビットの I ピクチャ、P ピクチャ、B ピクチャの識別フラグであり、その値が“00”の時は I ピクチャ、“01”の時は P ピクチャ、“10”の時は B ピクチャであることを示す。ここで、I ピクチャの場合は必ず記述が必要で、P または B ピクチャの場合は、オプションとし、必ずしも記述しなくてもよい。また、“Byte_position”は、I ピクチャ、P ピクチャ、および B ピクチャの先頭のファイルにおけるバイト位置を 32 bit で示す。さらに、“PB_number”は、或る I ピクチャから次の I ピクチャまでの間に存在する P ピクチャと B ピクチャの合計数を 5 ビットで示す。“Timestamp”は、I ピクチャ、P ピクチャ、B ピクチャの時刻情報で、それぞれの MPEG の I ピクチャまたは P ピクチャまたは B ピクチャを構成するタイムスタンプ付き TS 列の先頭など特定位置の TS のタイムスタンプ値を 40 ビットに変換して使用する。それぞれのパラメータ、フラグの値の定義は、前記の組合せに限定されない。

【0132】

以上により、きめ細かやで綺麗なスロー再生や高速再生などのトリック再生が実現できる。なお、このピクチャ情報ファイルはリモート端末からローカル端末内の異なるフォーマットで記録された MPEG-TS ファイル内のピクチャ位置を共通のファイル形式で見せることができるフィルタ機能として考えることができる。すなわち、独自のファイル形式で MPEG-TS を記録した AV データファイルとその関連情報ファイルより、共通のピクチャ情報ファイルを生成することができる。

【0133】

本発明で用いる入力データの適用範囲として、サーバー型放送や各社の異なる DRM 方式など一般の DRM 対応の AV コンテンツを DTCIP-I/P を用いて伝送することが可能となる。

【0134】

また、第 4 の実施例の構成により、AV コンテンツを AKE や暗号処理を実装しない送受信装置による実装の場合にも、MPEG の I ピクチャまたは P ピクチャまたは B ピクチャに効率よくアクセスできるという効果を得ることができる。

【0135】

さらに、本発明の別機能について説明する。図 4 のコンテンツバッファ 413 において、MPEG-TS 信号に、たとえばリードソロモン方式のエラー訂正符号を付加した後、暗号化手段 414 で暗号化する。これにより、送受信機器間で MPEG-TS 信号を DTCIP 方式により暗号化し、さらにエラー訂正符号を付加しリアルタイム伝送が可能となる。ここで、MPEG-TS のヘッダー付加および伝送処理のパケット化手段をハードウェ

アで構成すると、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい一般データの packets 化はマイコンなど安価なプロセッサで処理できる。

【産業上の利用可能性】

【0136】

本願によれば、デジタル放送やDVDディスクのコピー制限コンテンツを、コンテンツの著作権者によって設定されたコピー制御情報を継承しながらIPネットワークを用いて違法コピーを回避しつつ安全に伝送することが可能となる。たとえば、一般家庭において、1階の今にあるデジタルチューナーやDVDレコーダから2回の寝室にあるディスプレイに映画などのプレミアムコンテンツを伝送することが可能となる。

【図面の簡単な説明】

【0137】

- 【図1】 本願発明を適用するシステムの一例を示す図
- 【図2】 認証と鍵交換にDTC P方式を適用する場合のコンテンツ伝送手順の説明図
- 【図3】 イーサネット（登録商標）を用いる一般家庭に適用した場合の一例の説明図
- 【図4】 本願第1の発明および第2の発明の packets 送信手段のブロック図
- 【図5】 本願第1の発明のプロトコルスタックによる説明図
- 【図6】 本願第1の発明におけるMPEG-TSのイーサネット（登録商標）フレーム構成仕様の例を示す図
- 【図7】 本願第3の発明における packets 送受信手段の構成を示すブロック図
- 【図8】 本願第4の発明の packets 送受信手段の構成を示すブロック図
- 【図9】 従来例における送信システムの説明図
- 【図10】 従来例における送信機器および受信機器の構成を示すブロック図
- 【図11】 従来例における鍵交換にDTC P方式を適用する場合のコンテンツ伝送手順の説明図
- 【図12】 従来例における1395アイソクロナス packets の構成例を示す図
- 【図13】 ピクチャ情報ファイルの構成を示す図

【符号の説明】

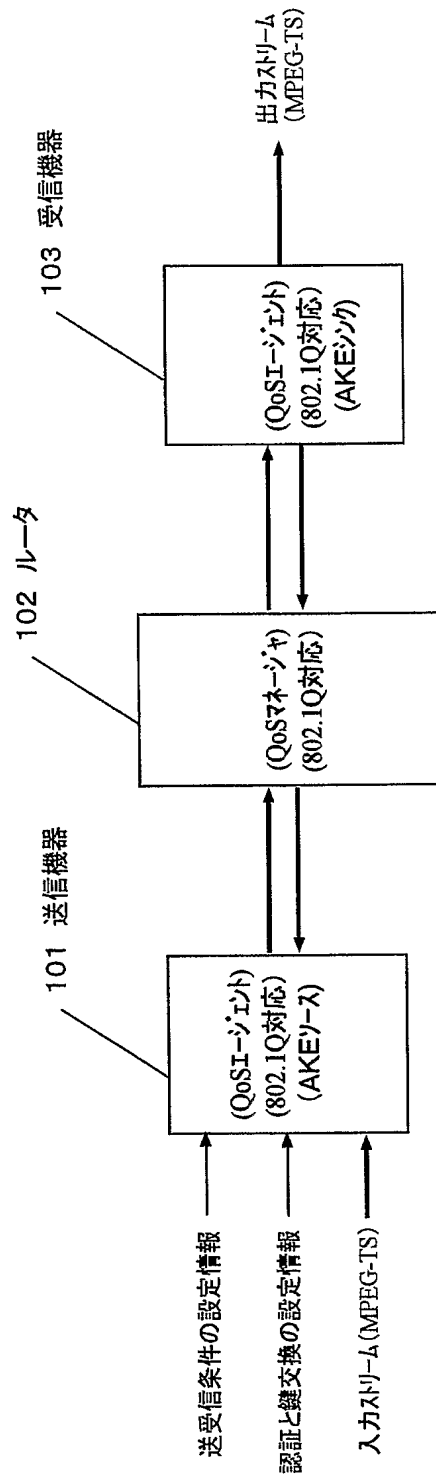
【0138】

- 101 パackets 送信機器
- 102 ルータ
- 103 パackets 受信機器
- 401 パackets 送信手段
- 402 TSストリーム識別手段
- 403 送信条件の設定管理手段
- 404 DRM設定管理手段
- 405 AKE手段
- 406 packets 化手段
- 407 暗号化データ復号手段
- 408 フレーム化手段
- 409 フレーム受信手段
- 410 packets 受信手段
- 411 DRMコンテンツ購入決済手段
- 412 コンテンツメタ情報
- 413 コンテンツバッファ
- 414 暗号化手段
- 415 暗号化情報ヘッダー付加手段
- 416 HTTP/ RTPヘッダー付加手段
- 417 送信条件の条件設定手段

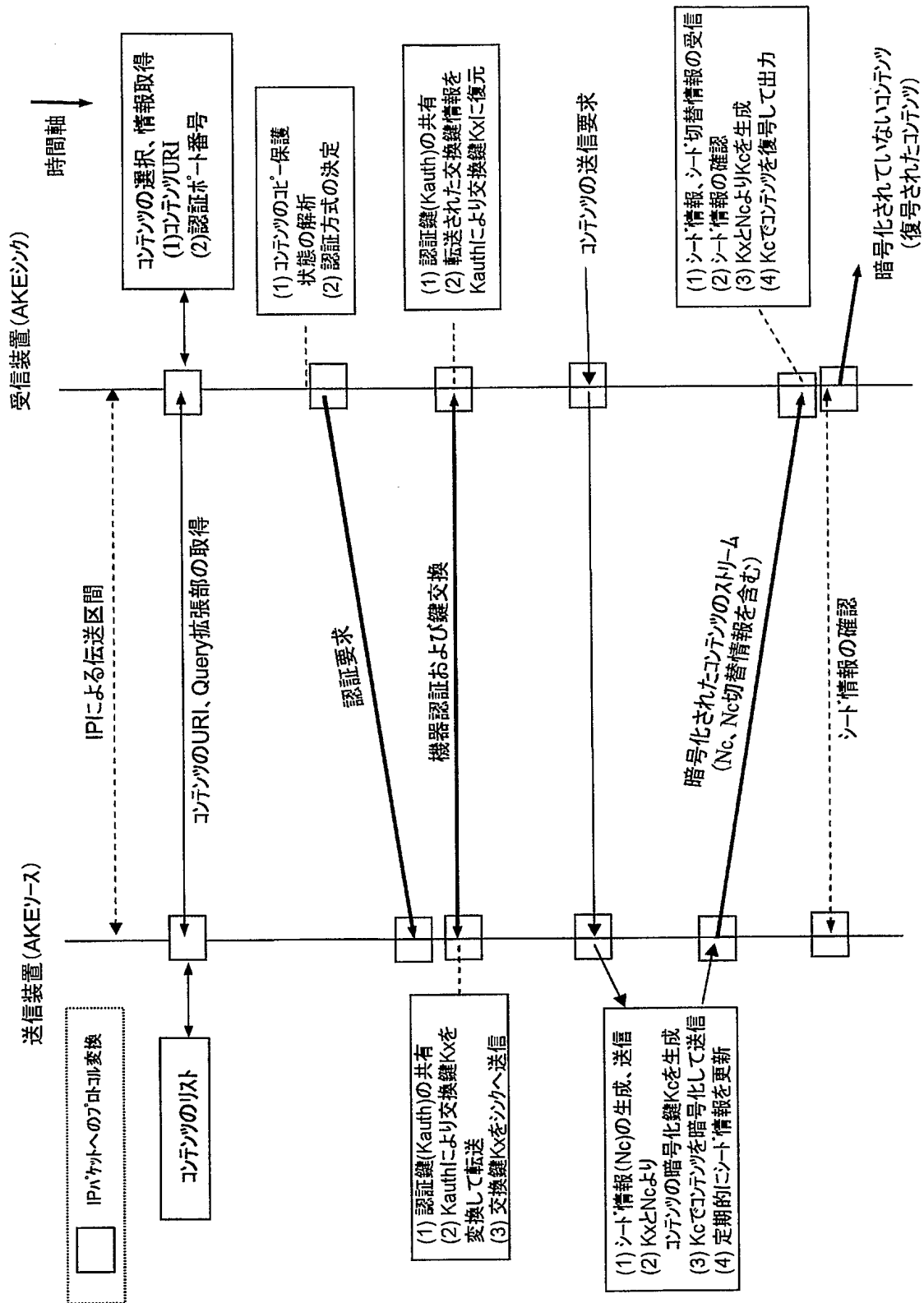
4 1 8 復号化手段
7 0 1 蓄積手段
8 0 1 I フレーム位置情報生成手段

【書類名】 図面

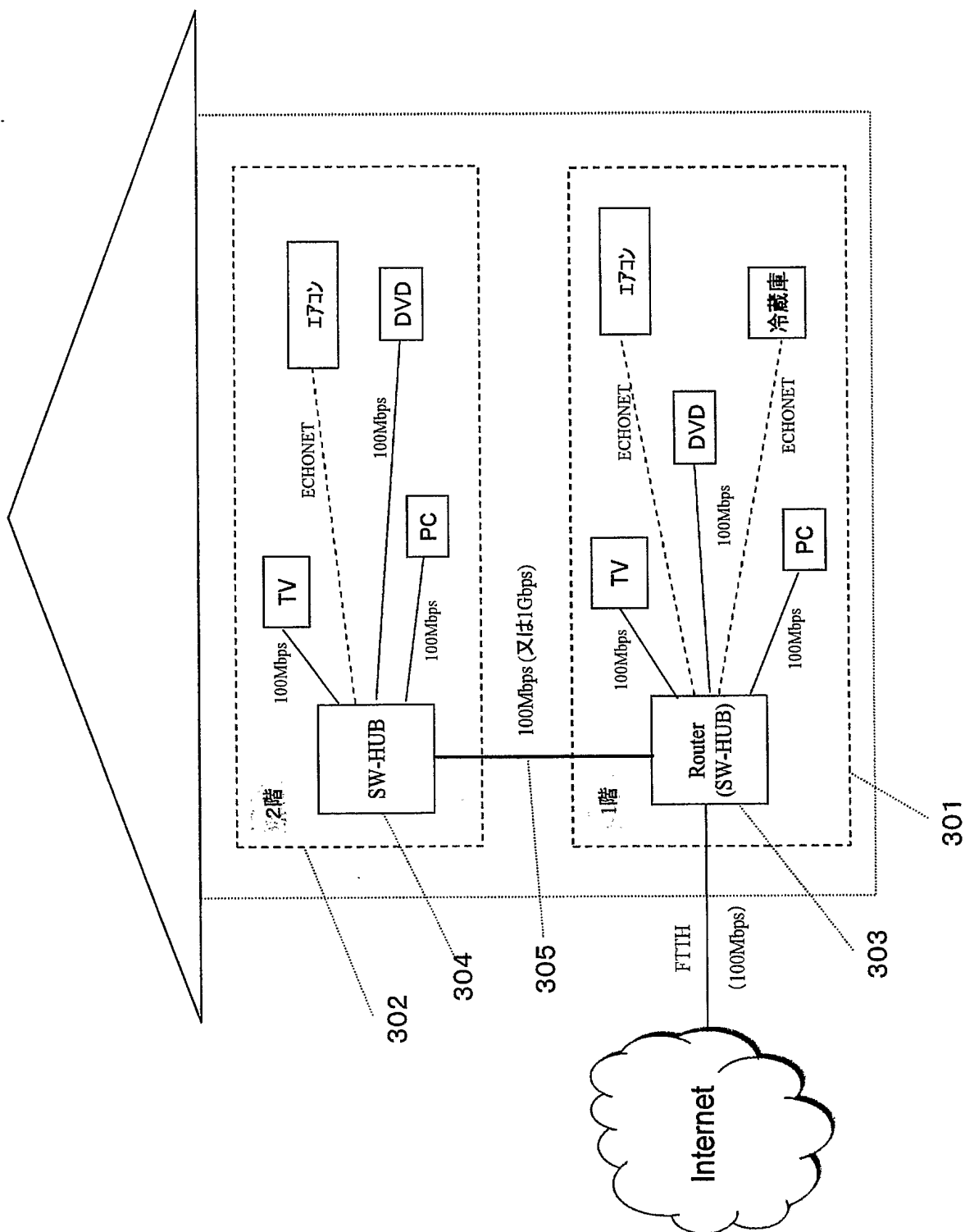
【図 1】



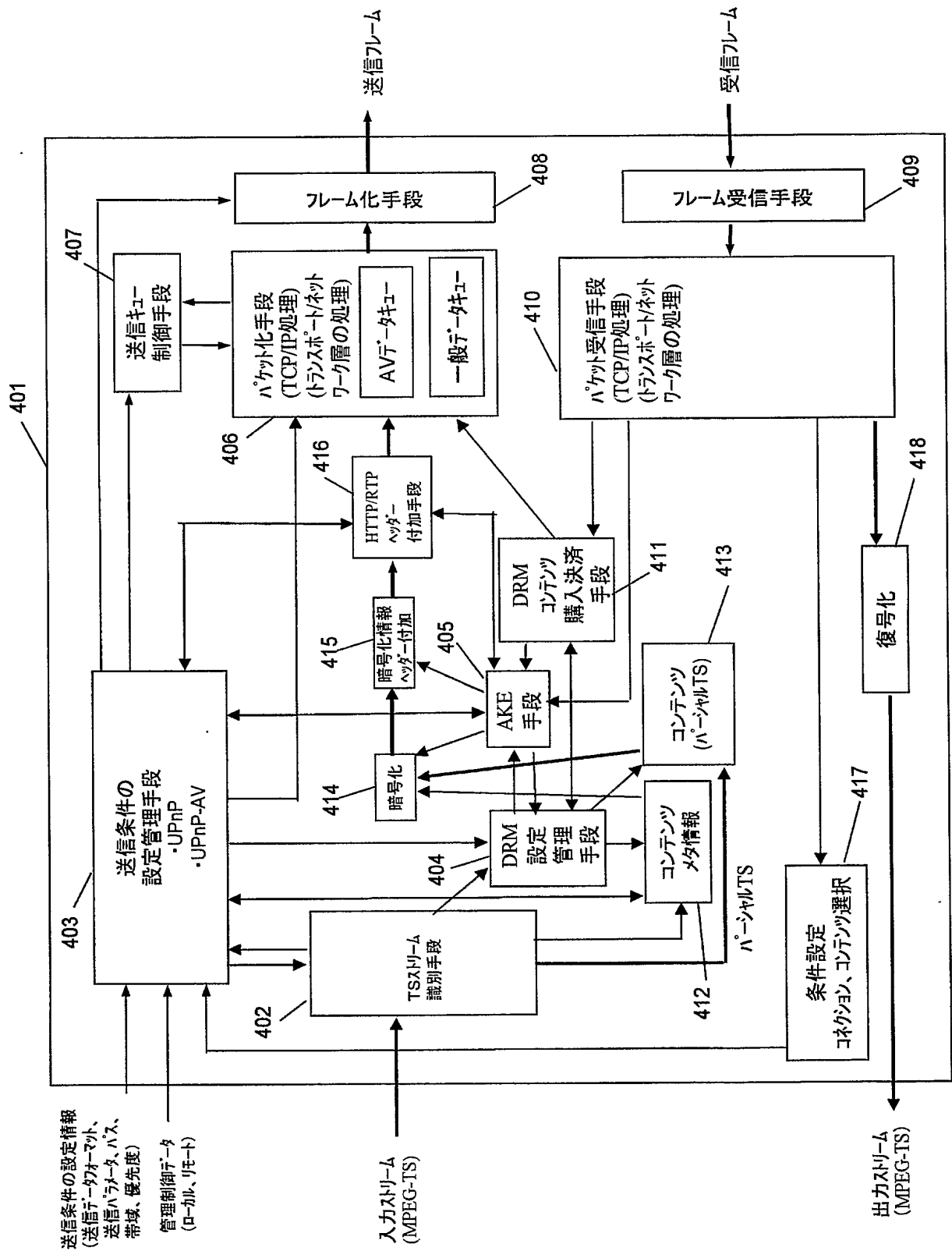
【図 2】



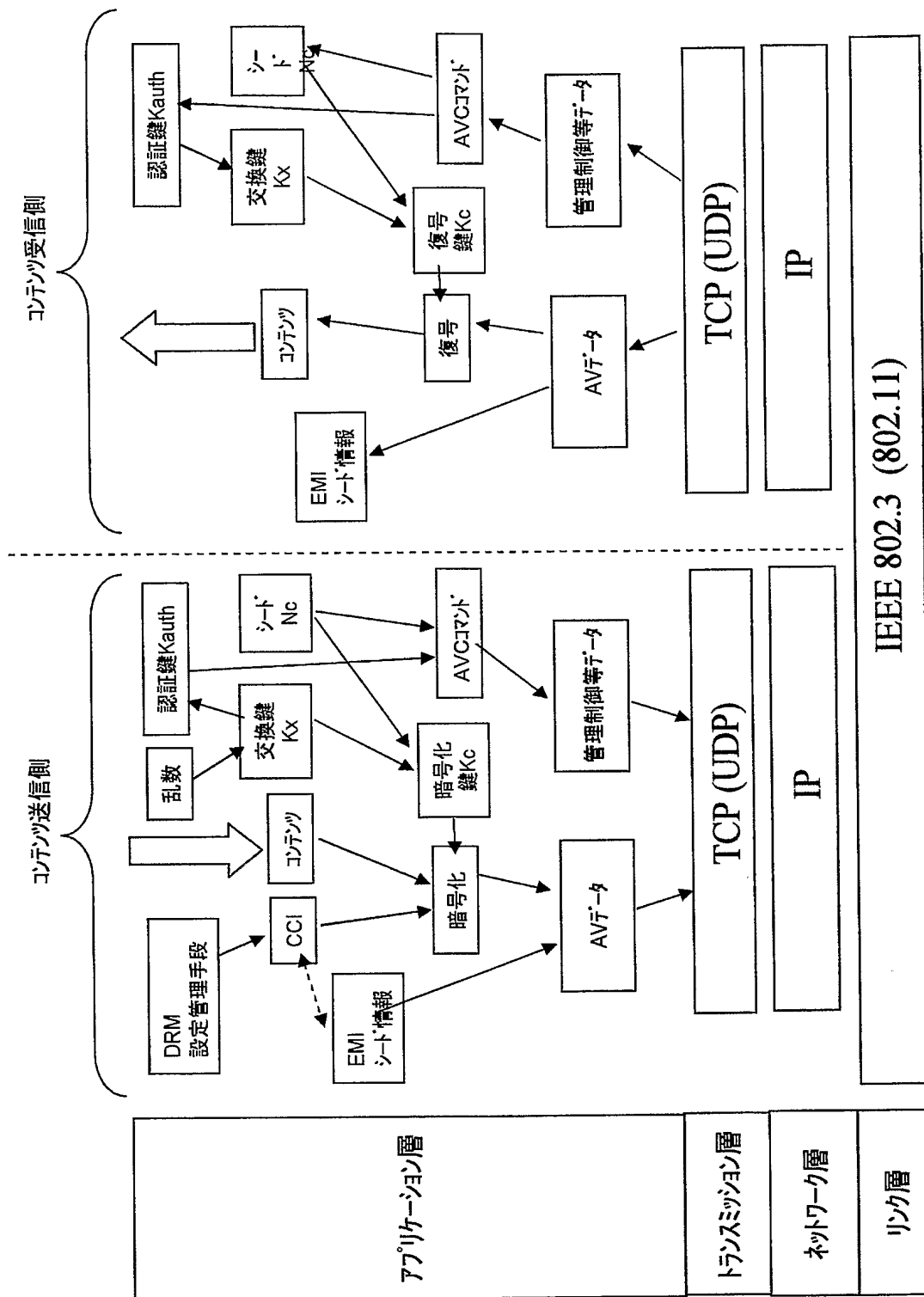
【図 3】



【図 4】

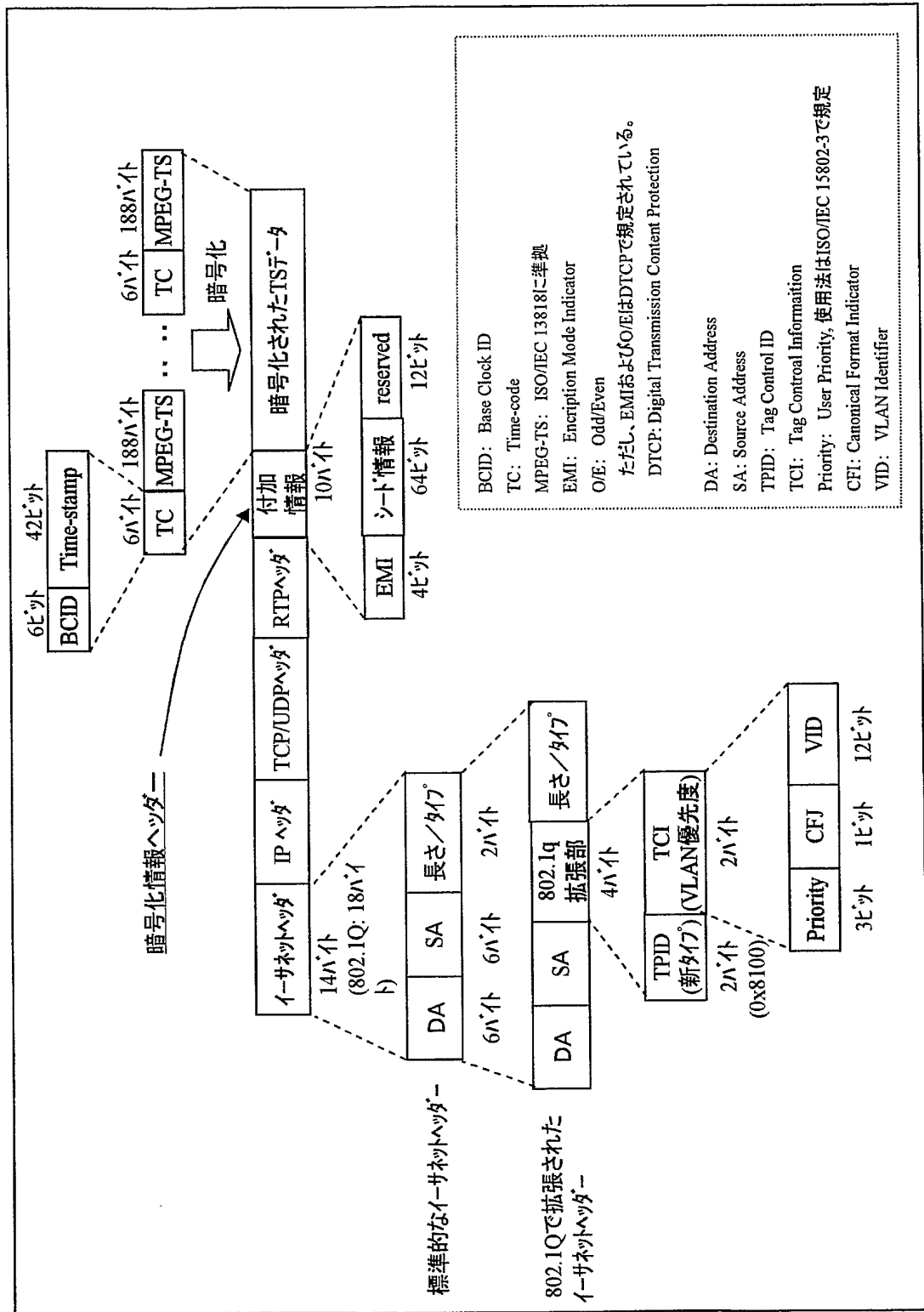


【図 5】

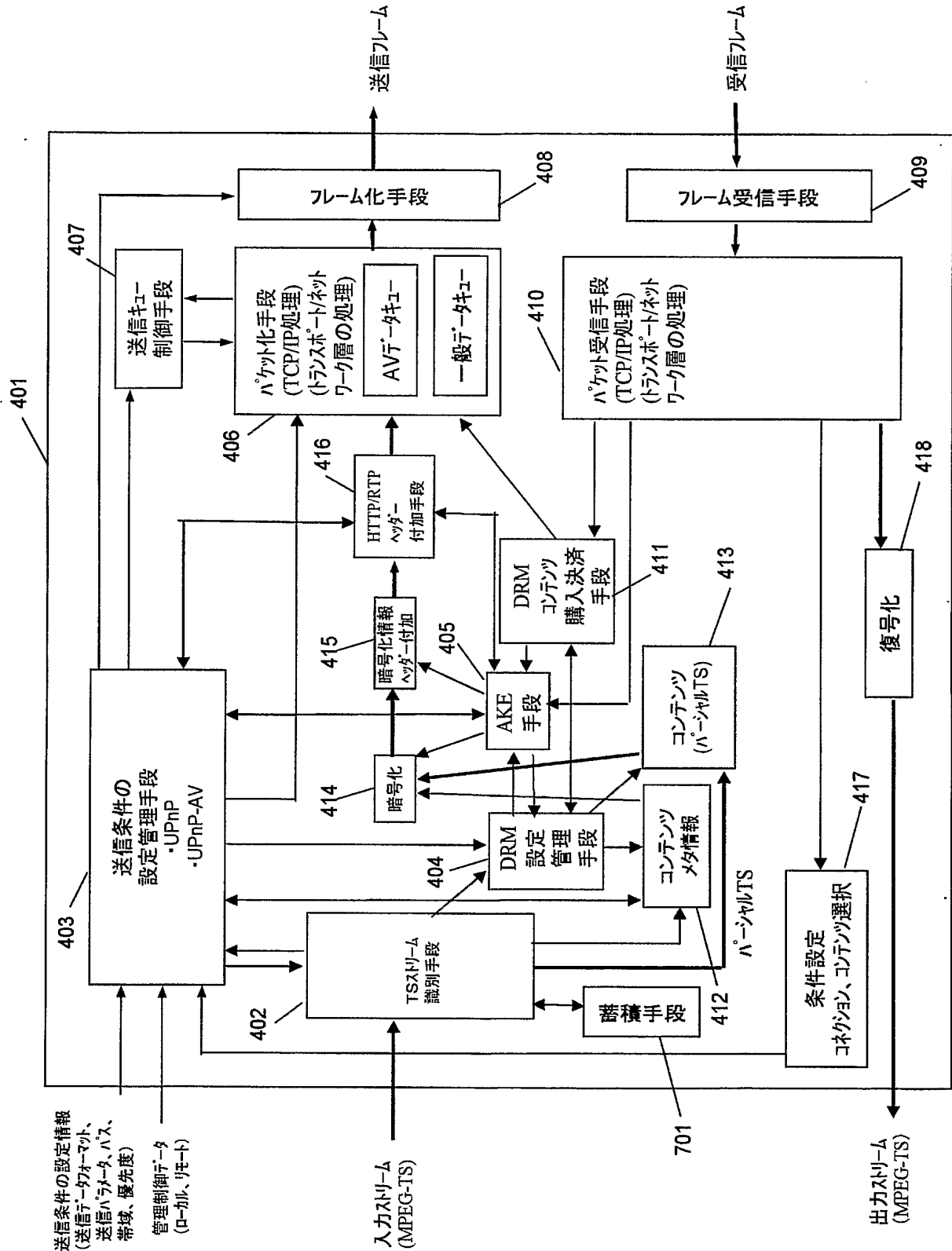


(OSIモデルによる説明)

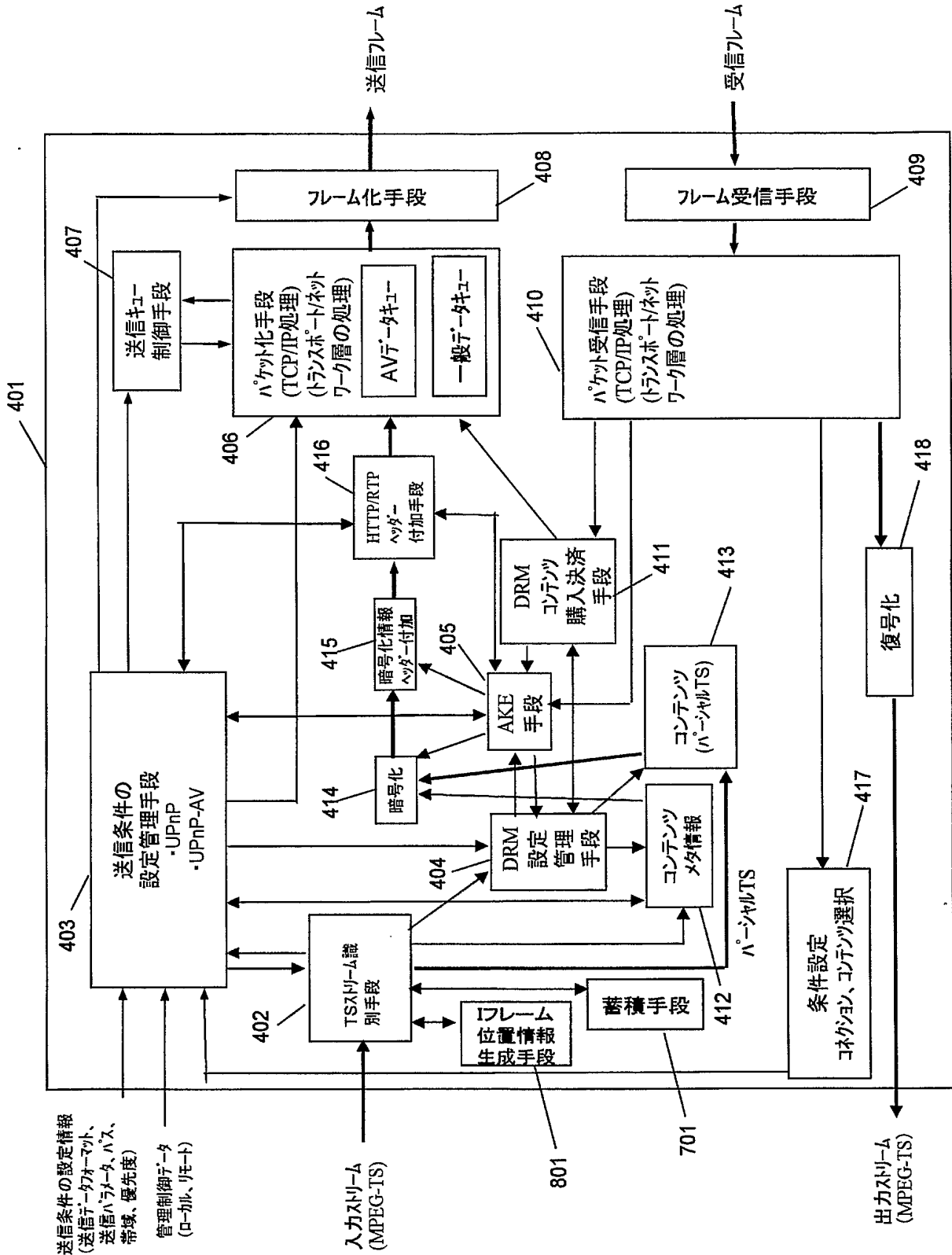
【図 6】



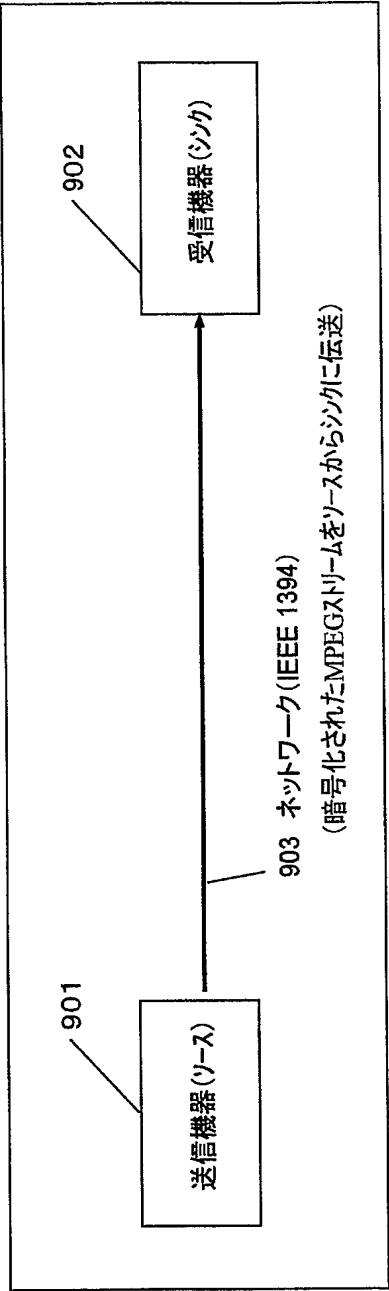
【図 7】



【図8】



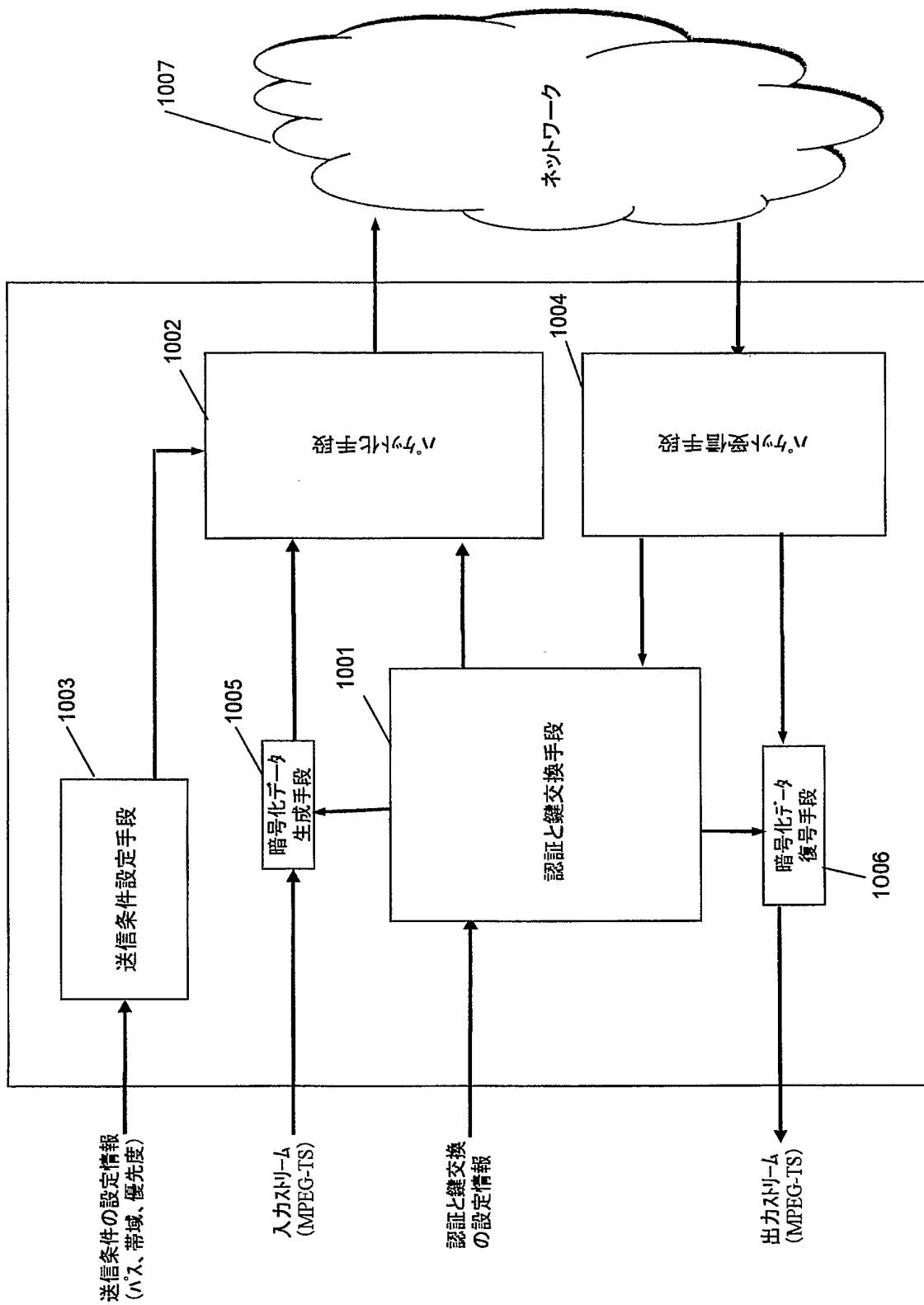
【図 9】



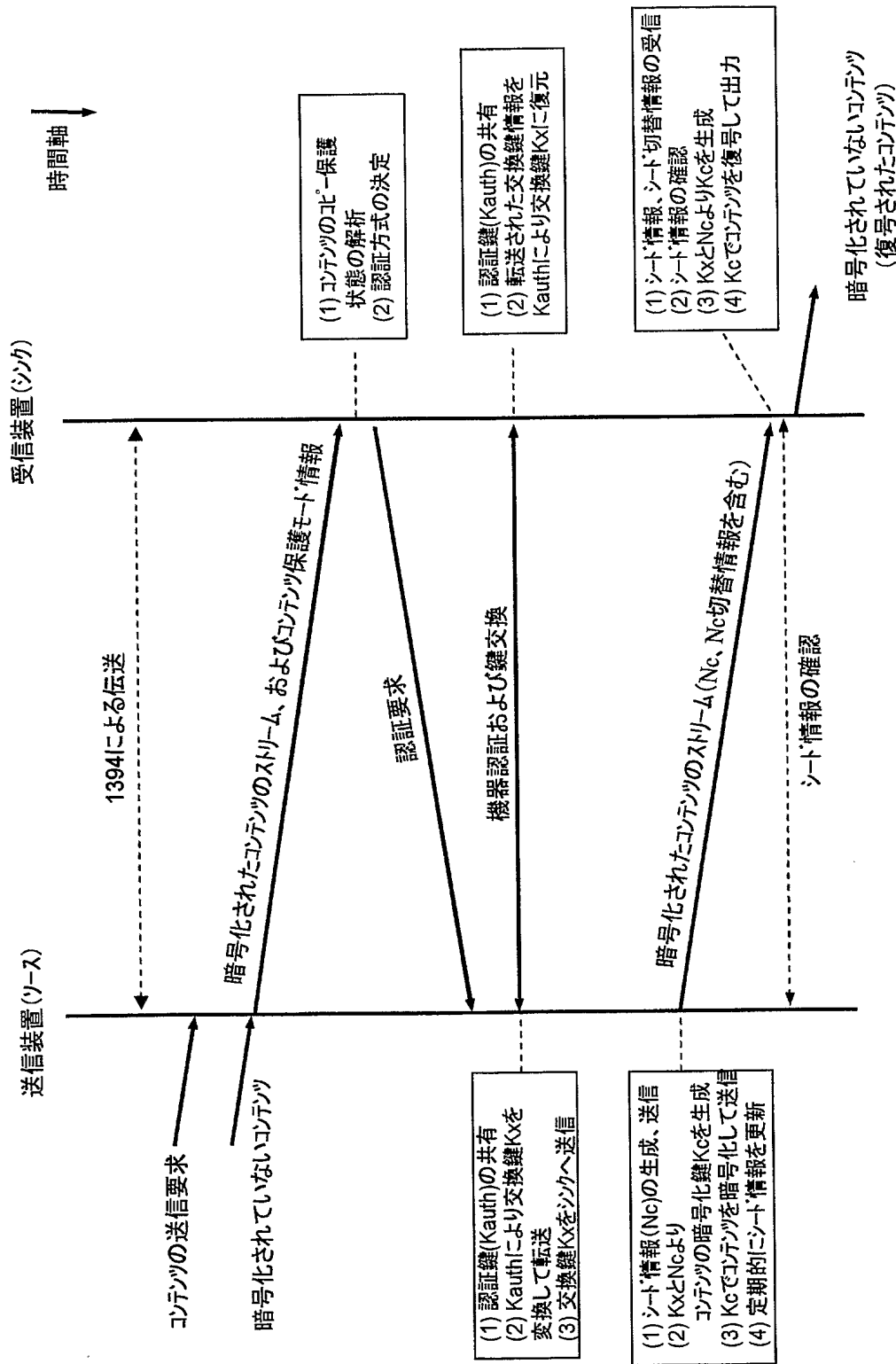
送信機器 (ソース) の例	受信機器 (シンク) の例	コンテンツ伝送における暗号化
DVHS	DVHS	MPEG-TSにDTCP方式 によるコンテンツ保護を実施
HDDレコーダ	HDDレコーダ	
1394搭載STB	1394搭載STB	
1394搭載デジタルTV	1394搭載デジタルTV	

IEEE 1394においてDTCPを用いたMPEGストリームの伝送

【図 10】

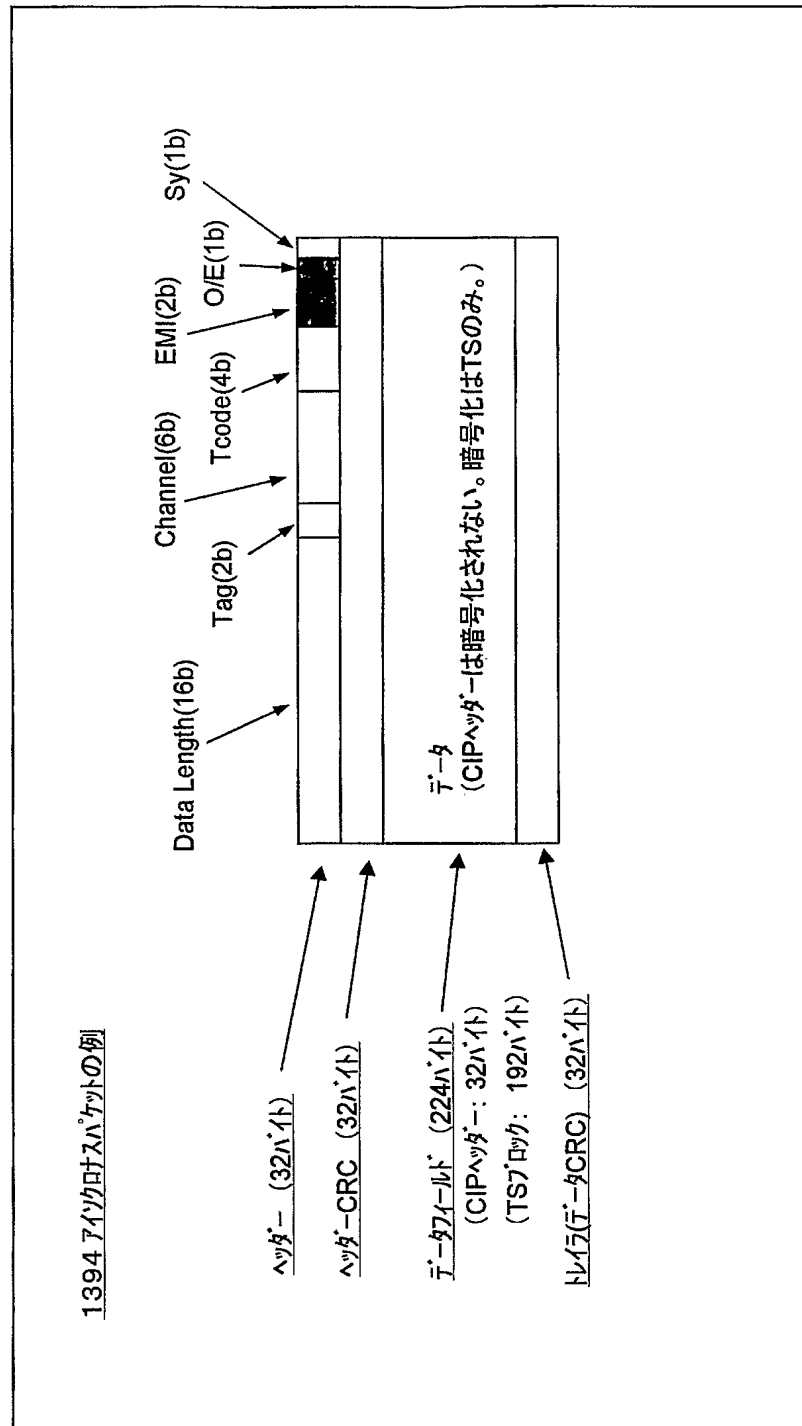


【図 11】



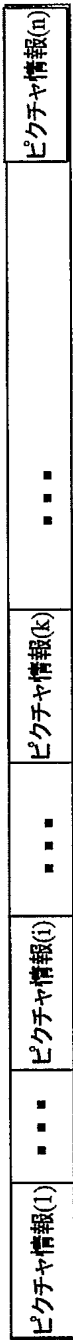
IEEE 1394においてDTCPを用いた暗号化ストリーム伝送手順(従来技術)

【図 12】



【図 13】

ピクチャ情報ファイル(PIF: Picture Information File)の構成



80ビット



2ビット



パージナルTSを記録したHDDやBDディスクなどから、I/P/Bピクチャの連続性、位置情報、時刻情報などを統一した「ピクチャ情報ファイル」に書き出す。ネットワークを介して離れた場所が存在する端末からは、このピクチャ情報ファイルを参照することにより、異なるTS記録フォーマットでも各ピクチャ位置が参照できる。これにより、きめ細かなスローや高速再生などが実現できる。

discont: パージナルTSパケットの不連続性フラグ。
1ビットで表す。“0”は連続、“1”は不連続の意味。

IPB: Iピクチャ、Pピクチャ、Bピクチャの識別フラグ
“00”はIピクチャ、“01”はPピクチャ、“10”はBピクチャの意味。

“00”のIピクチャ位置の記述は必須。
“01”のPピクチャおよび“10”のBピクチャの記載は任意(オプション)。

Byte_position: Iピクチャ、Pピクチャ、Bピクチャの先頭のファイルにおけるバイト位置。32bitで表す。

PB_number: 或るピクチャから次のIピクチャまでの間に存在するPピクチャとBピクチャの合計数。5bitで表す。

Timestamp: Iピクチャ、Pピクチャ、Bピクチャの時刻情報。
40bitで表す。

【書類名】 要約書

【要約】

【課題】 デジタル放送やサーバー型放送などの著作権保護されたMPEGコンテンツを、そのRMPIなどデジタル著作権情報を継承しつつ、IPネットワークを用いて伝送する手段を実現する。また、RMPやネットDRMに対応していない受信機においても視聴を可能とする。

【解決手段】 本願発明によるパケット送信手段は、AVデータとデジタル著作権管理情報などを夫々入力するデータ入力手段と、デジタル著作権情報をDTCPIP伝送の送受信条件に変換する手段と、暗号化または暗号化情報ヘッダー付加の実行を行う暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備する。また、異なるフォーマットに対して共通のIフレーム位置情報を生成する手段を具備するため、複数の蓄積フォーマットに対して効率のよい特殊再生を実現する。

【選択図】 図4

特願 2 0 0 4 - 2 6 1 0 3 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日 1 9 9 0 年 8 月 2 8 日

[変更理由] 新規登録

住 所 大阪府門真市大字門真 1 0 0 6 番地

氏 名 松下電器産業株式会社